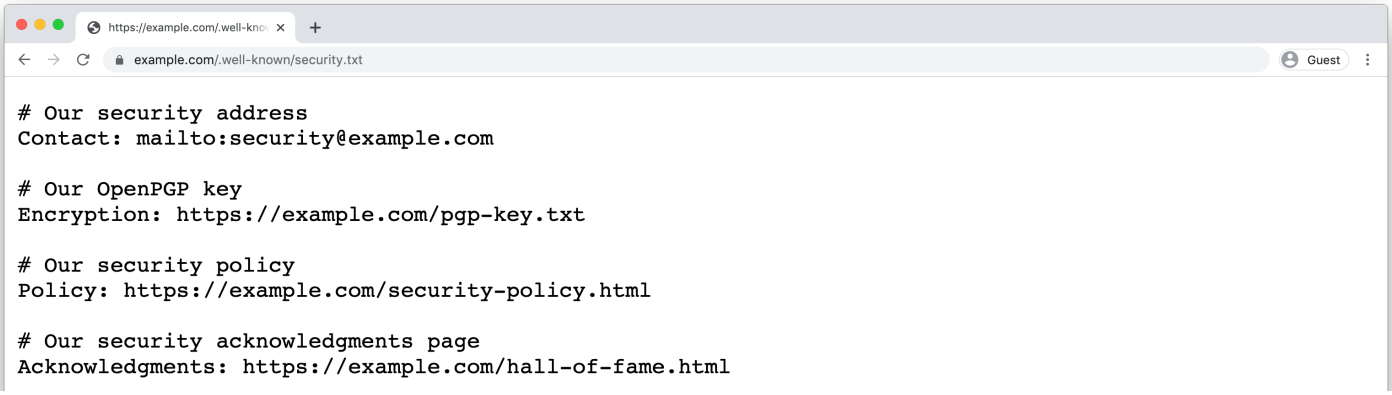
security.txt

A proposed standard which allows websites to define security policies.

Read the RFC → See it in action →

@securitytxt created by EdOverflow and Yakov Shafranovich



Summary

"When security risks in web services are discovered by independent security researchers who understand the severity of the risk, they often lack the channels to disclose them properly. As a result, security issues may be left unreported. security.txt defines a standard to help organizations define the process for security researchers to disclose security vulnerabilities securely."

`security.txt` files have been implemented by Google, Facebook, GitHub, the UK government, and many other organisations. In addition, the UK's Ministry of Justice, the Cybersecurity and Infrastructure Security Agency (US), the French government, the Italian government, the Dutch government, and the Australian Cyber Security Centre endorse the use of security.txt files.

Step 1

Create a text file called `security.txt` under the `.well-known` directory of your project.

Recent changes to the specification

The date format for Expires has changed to ISO 8601. An example of the new format is `Expires: 2021-12-31T18:37:07.000Z` .

Contact Required

A link or e-mail address for people to contact you about security issues. Remember to include "https://" for URLs, and "mailto:" for e-mails. See the full description of Contact

mailto:security@example.com

Add another alternative

Expires Required Only 1 allowed

The date and time when the content of the security.txt file should be considered stale (so security researchers should then not trust it). Make sure you update this value periodically and keep your file under review. See the full description of Expires

mm/dd/yyyy --:-- --

Add another alternative

Encryption Optional

A link to a key which security researchers should use to securely talk to you. Remember to include "https://". See the full description of Encryption

https://example.com/pgp-key.txt

Add another alternative

Acknowledgments Optional

A link to a web page where you say thank you to security researchers who have helped you. Remember to include "https://". See the full description of Acknowledgments

https://example.com/hall-of-fame.html

Add another alternative

Preferred-Languages Optional Only 1 allowed

A comma-separated list of language codes that your security team speaks. **You may include more than one language**. See the full description of Preferred-Languages

en, es, ru

Add another alternative

Canonical Optional

The URLs for accessing your security.txt file. It is important to include this if you are digitally signing the security.txt file, so that the location of the security.txt file can be digitally signed too. See the full description of Canonical

https://example.com/.well-known/security.txt

Add another alternative

Policy Optional

A link to a policy detailing what security researchers should do when searching for or reporting security issues. Remember to include "https://". See the full description of Policy

https://example.com/security-policy.html

Add another alternative

Hiring Optional

A link to any security-related job openings in your organisation. Remember to include "https://". See the full description of Hiring

https://example.com/jobs.html

Add another alternative

Generate security.txt file

Step 2

You are ready to go! Publish your security.txt file. If you want to give security researchers confidence that your security.txt file is authentic, and not planted by an attacker, consider digitally signing the file with an OpenPGP cleartext signature.

Copy to clipboard

Frequently asked questions

What is the main purpose of security.txt?

The main purpose of security.txt is to help make things easier for companies and security researchers when trying to secure platforms. Thanks to security.txt, security researchers can easily get in touch with companies about security issues.

Is security.txt an RFC?

Yes! We welcome contributions from the public: https://github.com/securitytxt/security-txt

Where should I put the security.txt file?

For websites, the security.txt file should be placed under the `/.well-known/` path (`/.well-known/security.txt`) [RFC8615]. It can also be placed in the root directory (`/security.txt`) of a website, especially if the `/.well-known/` directory cannot be used for technical reasons, or simply as a fallback. The file can be placed in both locations of a website at the same time.

Are there any settings I should apply to the file?

The security.txt file should have an Internet Media Type of `text/plain` and must be served over HTTPS.

Will adding an email address expose me to spam bots?

The email value is an optional field. If you are worried about spam, you can set a URI as the value and link to your security policy.

Video summary

LiveOverflow produced a video summarising the most important facts surrounding `security.txt` files. **Please note:** the video was produced on April Fool's Day and therefore includes a few tongue-in-cheek comments about people getting LiveOverflow and EdOverflow mixed up.